2021

Data Protection Policy

incorporates data collection, processing, sharing, storage and protection

WEBS Training Ltd
The Poplars
Wollaton Road
Beeston
Nottingham
NG9 2PD

01159 677771
www.webstraining.com

Data Protection Policy

Date: 14/01/2021

Purpose of Policy: Sets out the arrangements for Data collection, submission, sharing, storage and protection.

Approved by: Nick Crowther (Chair of the Board of Directors)

Responsibility for Updates: Lorraine Jameson (Head of Business & Quality Assurance)

Policy applies to: All WEBS employees, board members, learners, parents/carers, employers, third part organisations, suppliers and other individuals with whom WEBS work with.

Version no: 8

Proposed Date of Review: January 2021

Version History			
Version	**Date**	**Detail**	**Author**
2	03/03/16	Review and Update	Sammy Jones
3	31/07/17	Review and Update	Sammy Jones
4	17/03/18	Updated to Inc. GDPR	Sammy Jones
5	16/05/18	Updated following feedback	Sammy Jones
6	23/07/19	Review	Sammy Jones
7	08/01/20	Review & Update	Lorraine Jameson
8	14/01/21	Review & Update	Lorraine Jameson

Links and Dependencies

This policy is part of a suite of support policies aimed at supporting confidentiality of information.

- Access to Personal Data Files Policy & Procedure
- Complaints Policy
- Confidentiality Policy
- Data Breach Procedure
- Disciplinary Policy
- Learner E Safety Policy
- Health & Safety Policy
- Information Incident Response Plan
- Information Security Policy
- Preventing Radicalisation Policy
- Privacy Notice
- Record Retention Policy
- Safeguarding Policy
- Staff Induction Procedures
- Subject Access Request Procedures
- WEBS Continuity Plan
- Whistleblowing Policy

This list is not exhaustive. A copy of our policies can be obtained on request.

Contents Page

Policy Statement

WEBS Training Ltd is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

WEBS Training Ltd, as part of its employment and training function has to collect and retain certain information about its staff, apprentices, employers, board members suppliers and other individuals for a variety of business and contractual purposes.

This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Champion (DPC) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Definitions

Business purposes	The purposes for which personal and sensitive data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. *Business purposes include the following:* - *Compliance with our legal, regulatory and corporate governance obligations and good practice* - *Compliance with our contractual relationships with the Education & Skills Funding Agency, Awarding Bodies, End Point Assessment Organisations in meeting the requirements of an Approved Apprentice Training Provider* - *Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests* - *Ensuring business policies are adhered to (such as policies covering email and internet use)* - *Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information and security vetting* - *Investigating complaints* - *Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments* - *Monitoring staff conduct, disciplinary matters* - *Marketing our business* - *Improving services*

WEBS regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between WEBS and those with whom it carries out business. WEBS will ensure that it treats personal and sensitive information lawfully and correctly.

To this end WEBS fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998 and the new General Data Protection Regulation (GDPR) implemented in the UK from 25 May 2018 and further identified below.

Scope

This policy applies to all staff, who must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Any breach of the Data Protection Act 1998/GDPR, or the WEBS Data Protection Policy is considered to be an offence and in that event, disciplinary procedures will apply in line with WEBS policies.

Background to the Data Protection Act 1998 and GDPR

The purpose of the Data Protection Act 1998 is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

In May 2018 the European General Data Protection Regulations (GDPR) came into force to protect the personal data of EU citizens. This replaces the Data Protection Act and will broaden the scope of the current data protection framework in line with today's technological changes. It brings further rights to individuals including giving data subjects more control over their data and introduces a formal and timely notification procedure for any breaches of data.

Throughout this policy, reference to the 'Act' shall mean the Data Protection Act 1998 up to 24 May 2018 and thereafter shall refer to the new General Data Protection Regulations.

Definitions

Personal Data
Personal Data has been redefined under GDPR. Where personal data was previously defined in the DPA as a person's name, photo, email address, phone number, address, or any personal identification number (social security, bank account, etc.), it will have a much broader definition under the GDPR. Under the GDPR things like IP addresses, mobile device identifiers, geolocation and biometric data (finger prints, retina scans, etc.) will constitute personal data. In addition an individual's physical, psychological, genetic, mental, economic, cultural, or social identity are also covered by the GDPR.

Sensitive Personal Data
Special categories of personal data (such as name, address, telephone) and includes genetic and biometric data where processed to uniquely identify and individual.

Data Controller
Any person (or organisation), which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by law.

Data Processor
Processes data on behalf of the controller.

Processing
Any operation related to organisational and technological process including retrieval, disclosure and deletion of data and includes: obtaining and recording data accessing, altering, adding to, merging or deleting data.

Data Subject
Any living individual who is the subject of personal data held by an organisation.

Supervisory Authority
This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.

The Principles

The Act stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.

We will make sure the information is:

- Processed lawfully, fairly and in a transparent manner
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate and kept up to date
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the UK without adequate protection

In addition GDPR defines a further principle around accountability requiring an organisation to show how it complies with the eight principles identified above.

Data Protection Risks

This policy helps to protect WEBS Training Ltd from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them (exceptions apply, refer to individual rights).
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Individual Rights

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist and includes:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure or the right to be 'forgotten'
- The right to restrict processing

- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

However, data subjects must note that there are a number of circumstances where WEBS does not have to comply with certain rights, for example:

- a request for access to personal data where disclosure of information refers to another individual who can be identified from that information.
- A request to delete data where we are processing to comply with a lawful basis

Our Procedures

Fair & Lawful Processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal and sensitive data unless the individual whose details we are processing has consented to this happening.

If we cannot apply a lawful basis (explained below), our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased

Controlling vs Processing

WEBS Training Ltd is classified as a data controller and data processor. We must maintain our appropriate registration with the Information Commissioners Office in order to continue lawfully controlling and processing data.

As a data processor, we must comply with our contractual obligations and act only on the documented instructions of the data controller. If we at any point determine the purpose and means of processing out with the instructions of the controller, we shall be considered a data controller and therefore breach our contract with the controller and have the same liability as the controller. As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

Lawful Basis for Data Processing

1. Contractual Obligation

Processing of employee data is necessary in relation to individual employment contracts and to comply with an employer's legal obligations such as:

- recruitment, equality of opportunity, payment of salaries, pensions, tax, training, staff appraisals etc.;

Processing of learner data is necessary to comply with Education and Skills Funding Agency contracts:

- To confirm eligibility to Apprenticeship/Traineeship programmes
- To fund apprenticeship delivery
- To monitor equality of opportunity
- To provide appropriate support

Data may be used for statistical purposes in relation to reporting achievements, success rates, retention, attendance etc.

2. Legal Obligation

Processing of employee data is necessary for compliance with employment law and safeguarding e.g. to carry out DBS checks

Processing of apprentice/learner data to meet legal responsibilities and compliance under the Apprenticeship, Skills, Children and Learning Act 2009.

3. Legitimate Interest

The processing of employee and learner data is necessary in relation to good governance, accounting, managing and auditing business operations in addition to any potential safeguarding concerns.

4. Vital interests

Processing the data is necessary to protect a person's life or in a medical situation.

5. Public function

Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.

6. Consent

For the purposes of marketing, employee and learner personal data or sensitive data will not used or disclosed unless the individual has given consent.

WEBS Training Limited understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them.

Consent obtained under duress or on the basis of misleading information is not a valid basis for processing. From 25 May 2018, Data subjects are required to 'opt-in' via a signed consent form which will be held in the data subjects personnel/evidence file. Consent will not be inferred from non-response to a communication.

For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists e.g.vital interest such as safeguarding.

In most instances consent to process personal and sensitive data is obtained routinely by WEBS Training Ltd (e.g. when a Learner signs an individual learning plan/consent form or when a new member of staff signs a contract of employment).

Any WEBS forms (whether paper-based or web-based) that gather data on an individual will contain a statement explaining what the information is to be used for and to whom it may be disclosed.

If an individual does not consent to certain types of processing (e.g. for direct marketing), appropriate action must be taken to ensure that the processing does not take place.

If any staff member is in any doubt about these matters, they should consult the Management Information and Data Officer.

Deciding which condition to rely on

When making an assessment of the lawful basis, WEBS will first establish that the processing is necessary. This means the processing must be a targeted, appropriate way of achieving the stated purpose. We cannot rely on a lawful basis if we can reasonable achieve the same purpose by some other means. In some instances more than one basis may apply and we will identify the best fit the purpose taking into account the following factors:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are we in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are we able to stop the processing at any time on request, and have we factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

Special Categories of Personal Data

What are special categories of personal data?

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin

- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sexual orientation

In most cases where we process special categories of personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure contractual requirements or health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Responsibilities

As the Data Controller WEBS Training Ltd is responsible for establishing policies and procedures in order to comply with the requirements of the Data Protection Act 1998/GDPR.

1. Board Responsibilities

The Board holds responsibility for:

- WEBS's Data Protection notification. Details of WEBS notification are published on the Information Commissioner's website. Anyone who is, or intends, processing personal data for purposes not included in the notification should seek advice from the Board;
- Approving guidance, giving advice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information;
- Advising on and ensuring that any data protection breaches are resolved, catalogued and reported appropriately in a swift manner and in line with guidance from the Information Commissioner's Office;
- Investigating and responding to complaints regarding data protection including requests to cease processing personal data.
- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Ensuring consent procedures are lawful
- Implementing and reviewing procedures to detect, report and investigate personal data breaches
- the provision of data protection training and awareness for staff
- ensuring that everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- for the development of best practice guidelines.
- ensuring that anyone wanting to make enquiries about handling personal information, whether a member of staff, an apprentice or a member of the public, knows what to do;
- ensuring that queries about handling personal information are promptly and courteously dealt with;

- ensuring that the methods of handling personal information are regularly assessed and evaluated;
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

2. The Data Protection Champion, is responsible for:

- Arranging data protection training and advice for staff.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data that WEBS holds about them (also called 'subject access requests').
- for carrying out compliance checks to ensure adherence, throughout WEBS, with the Act.
- Reviewing all data protection procedures and policies on a regular basis

3. Responsibilities of IT Service Provider

    - Ensure all systems, services, software and equipment meet acceptable security standards
    - Checking and scanning security hardware and software regularly to ensure it is functioning properly
    - Researching third-party services, such as cloud services the company is considering using to store or process data

4. Staff responsibilities

Staff members who process personal data about students, staff, applicants, alumni or any other individual must comply with the requirements of this policy.

Staff members must ensure that:

- all personal data is kept securely;
- no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- personal data is kept in accordance with the WEBS retention schedule;
- any queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPC.
- any data protection breaches are swiftly brought to the attention of the DPC and that they support the Board in resolving breaches;
- where there is uncertainty around a Data Protection matter advice is sought from the Board.

When members of staff are responsible for supervising learners doing work which involves the processing of personal information (for example in research projects), they must ensure that those learners are aware of the Data Protection Principles, in particular, the requirement to obtain the data subject's consent where appropriate.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the DPC.

5. Third Parties

Where external companies are used to process personal data on behalf of WEBS Training Ltd, responsibility for the security and appropriate use of that data remains with WEBS.

Where a third-party data processor is used:

- a data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- reasonable steps must be taken that such security measures are in place;
- a written contract establishing what personal data will be processed and for what purpose must be set out;
- a data processing agreement must be signed by both parties.

For further guidance about the use of third-party data processors please contact the DPC.

6. Learner responsibilities

Learners are responsible for:

- familiarising themselves with the Data Protection Agreement provided when they commence an apprenticeship/ training programme with WEBS Training Ltd;
- ensuring that their personal data provided to WEBS Training Ltd is accurate and up to date.
- Informing WEBS of any changes to information, which they provide, for example, change of address.

Accuracy & Relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPC.

Data Security

Effective data protection relies on organisations adequately protecting their IT systems from malicious interference. In implementing the GDPR standards, WEBS has evaluated the risks of processing such data and implemented appropriate measures to mitigate those risks.

Where other organisations process personal data as a service on our behalf, the Board of Directors in conjunction with the DPC will establish what, if any, additional specific data security arrangements need to be implemented in contracts/agreements with those third party organisations.

Securing Data Securely

All managers and staff at WEBS Training Ltd will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment where unauthorised personnel cannot access it;
- Personal data held on computers and computer systems is protected by the use of limited access and secure passwords, which have forced changes periodically (refer to WEBS Password Policy). We encourage all staff to use a password manager to create and store their passwords.
- Printed data should be shredded when it is no longer needed
- Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used
- The Board of Directors must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software
- All possible technical measures must be put in place to keep data secure

Data Reporting

Data may be used from time to time for organisational reporting, for example, to monitor employment trends, provide headcount, recruitment, absence and turnover statistics with regard to staffing matters. Alternatively, reports on progression destinations, retention, attendance and achievements are likely to be reported for learner matters. These will be based on statistical analysis and unlikely to contain personal data which would identify any one particular learner.

Data Retention

WEBS will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Disposal of Personal Data

Personal data will be securely disposed of when no longer needed. This reduces the risk that it will become inaccurate, out of date or irrelevant.

For hard copy data, disposal may be through a third party organisation for shredding of large amounts of records.

Data Breaches

What Constitutes a Data Protection Breach?
"A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This means that a breach is more than just losing data".

Where a Data Protection breach occurs, or is suspected, it should be reported immediately in accordance with the Breach Reporting Procedure.

Confirmed or suspected data security breaches should be reported promptly to the DPC as the primary point of contact on **0115 9677771** or email to data@webstraining.com. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved.

Any breach will be reported to the ICO within 72 hours where it is likely to result in a risk to the rights and freedoms of an individual and may cause harm and distress where there may be the potential for example, for fraudulent activity. In these cases, data subjects will also be informed.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the [name of supervisory authority] of any compliance failures that are material either in their own right or as part of a pattern of failures

Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our Breach Procedure for our reporting procedure.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. WEBS Training Limited is registered as such. Our ICO Registration number is Z7002117 and due for renewal on 31 July 2021. WEBS's data protection registration can be viewed at ico.org.uk

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

To this end the designated officers will be responsible for notifying and updating the Information Officer of the processing of personal data, within their area. The Information Officer will review the Data Protection Register with designated officers annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days. To this end, any changes made between reviews will be brought to the attention of the Information Officer immediately

The Privacy Notice

All staff and learners will be given a copy of the WEBS Privacy notice. The privacy notice will

inform staff and learners how their personal information will be processed and used including reference to third party organisations such as the Education Funding Agency (and any successor bodies to these offices) to fulfil statutory purposes, and by other bodies with whom data is shared for other legitimate purposes.

Access to Personal Data (Subject Access)

To obtain a copy of information held about you, to whom the Act applies, please refer to the WEBS Subject Access Procedures which can be found on the WEBS Sharepoint, Student shared drive or can be requested from WEBS directly. Please note that where a request is manifestly unfounded or excessive Inc. repetitive requests, WEBS has the right to refuse to respond. In such cases, WEBS will notify the data subject and notify the right to complain to the ICO at https://ico.org.uk/concerns/

Individuals will not be entitled to access information to which any of the exemptions in the Act applies. However, only those specific pieces of information to which the exemption applies will be withheld and determining the application of exemptions will be made by the Board.

Confidentiality

WEBS Training Ltd requires all members of staff to comply with the Act in relation to the information it holds. Failure to maintain confidentiality e.g. unauthorised, inappropriate or excessive disclosure of or obtaining information about individuals, will be regarded as serious misconduct and will be dealt with in accordance with the WEBS disciplinary policy and procedure.

Where a member of staff has specific responsibility for the management of personal sensitive data they will be given additional guidance on their obligations. However, members of staff must ask if they are unsure.

WEBS Training Ltd operates a whistle blowing policy which gives effect to our wish that no member of staff should feel reluctant for fear of management's response, to give information about any wrongdoings within WEBS.

Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by all employees at WEBS Training Ltd in relation to this policy, the Data Protection Champion will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess compliance with this Policy in relation to the protection of Personal Data, including:

- The assignment of responsibilities.
- Raising awareness.
- Training of Employees

The outcome of compliance monitoring will be reported at the Board meetings and any necessary action will be taken.

Contact

Queries regarding this policy or the Data Protection Act at large should be directed to the DPC or the Data Protection Champion at WEBS Training Ltd, The Poplars, Wollaton Road, Beeston, Nottinghamshire NG9 2PD or you can email at data@webstraining.com

Appendix 1 Data Records – Staffing

Data Controller The Chairman
WEBS Training Ltd
The Poplars
Wollaton Road
Beeston
Nottingham
NG9 2PD

Third Party Data Processors – Mabe Allen (Payroll); Royal London (Pensions); Blue Spire (Financial Advisor); Peninsula (HR); Friends Life (Life Assurance);

WEBS Training Ltd believes that the following list of records and their use are consistent with the employment relationship and principles of the DPA/GDPR. The information will be held for management and administrative use only, but there may be occasions when we need to disclose some information we hold to a relevant third party especially where we are legally obliged to do so (for example the Inland Revenue). We may also transfer information to another organisation, but this would be connected with an employee's career or due to the management of the employment relationship; for example to our external provider of payroll services so that staff may be paid.

Examples of information WEBS is responsible for:

- Information gathered about a member of staff and any references obtained during recruitment.
- Details of terms of employment
- DBS information.
- Payroll, tax and National Insurance information.
- Performance related information.
- Details of salary and job duties.
- Health records.
- Absence records, including holidays and self-certification forms.
- Details of disciplinary investigations and proceedings.
- Training records.
- Contact name and addresses.
- Any other information provided to WEBS in connection with employment.

Members of Staff are responsible for:

1. Ensuring that any information that they provide to WEBS in connection with their employment is accurate and up to date.
2. Informing WEBS of any changes to information, which they provide, for example, change of address.
3. If as part of their job, members of staff collect information about other living people, they must comply with this Data Protection Policy and Guidelines.
4. Ensuring that personal data is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff data is held in both electronic and paper formats.

Appendix 2 Data Records – Learners

Data Controller WEBS Training Ltd
The Poplars
Wollaton Road
Beeston
Nottingham
NG9 2PD

Data Processor Gareth Watson
Management Information and Data Officer

WEBS Training Ltd believes that the following list of records and their use are consistent with the learner relationship and principles of the Act.

Learner data is lawfully processed by WEBS in accordance with the terms and conditions of funding imposed by the Education and Skills Funding Agency (ESFA). The information will be held for our management, administrative and marketing use, together with disclosure of some of the information we hold to relevant third parties where we are obliged to do so (for example, awarding bodies, the Police where there may be safeguarding concerns, the Local Authority for their purpose of monitoring Raising of the Participation Age etc). When using learner data for marketing purposes, prior consent is sought.

Learner data will also be used in the matching of candidates to employer vacancies.

Learner data is held both manually in the form of applications, training records, ILP etc. and electronically via the Provider Integrated Clients System (PICS) and subject to electronic transfer to the Education & Skills Funding Agency for funding purposes.

Examples of learner information held by WEBS:

- Basic personal information gathered about a learner (name, address, gender, DOB)
- Sensitive information gathered about a learner (Ethnicity, Disability, Learning Difficulties)
- Learner photographs
- Details of a learner's programme of learning
- Examination details relating to a learner (entries and results)
- Attendance details for a learner
- Learner disciplinary records
- Information relating to school/career history and future destinations of learners on completion of their courses
- Case studies highlighting successful learners

For more information please refer to the learner Privacy Notice.

Appendix 3: Summary of Legal Requirements

Computer Misuse Act (1990)
This act safeguards against hacking and specifies 3 main offence areas.
Users will not:

- Use unauthorised access **–** for example, using another person's username and password, either with or without their permission; impersonation via email; attempting to access another user's files without their express permission, copying of software;
- Use unauthorised access with intent – for example, accessing financial, administrative or examination data without authorisation;
- Make unauthorised modification – for example, deliberately destroying or changing software or another user's files; changing data, or creating, introducing or transmitting a virus.

Maximum penalty for breach is up to 6 months imprisonment or up to a £5000 fine.

Data Protection Act (1998)
This act requires all members or agents of WEBS (staff, learners and associates) to abide by the terms of the WEBS's registration with the Data Protection Registrar. For any data held by WEBS, users must comply with the eight Data Protection Principles of good practice contained within the Act.

General Data Protection Regulations
This Act comes into force on 25 May 2018 and further enhances the Data Protection Act by strengthening the rights of individuals.

Obscene Publications Act (1959)
Protection of Children Act (1978)
Criminal Justice Public Order Act (1994)
These Acts specify the legal requirements for the protection of minors. Transmission or storage of pornographic, violent or offensive material is illegal for electronic as well as paper communications. Instances of such material found WEBS sites will be investigated and legal action will be taken.

Race Relations Act (1976)
This Act forbids discrimination against any person on the grounds of race or ethnic origin. It also provides protection against incitement to racial or ethnic discrimination. Thus, any material which either discriminates or encourages discrimination on racial or ethnic grounds is likely to contravene the Act and may lead to criminal prosecution of those responsible. Such information should not be stored or transmitted electronically.

Sex Discrimination Act (1975)
This Act forbids discrimination against any person on the grounds of gender, marital status inclusive of the advertising of material that may be discriminatory.

Public Order Act (1986)
Forbids material which encourages racial hatred or in any way threatens or insults others or may be considered abusive.

Equal Opportunities (Full Participation) Act (1995)
This Act forbids discrimination against any person on the grounds disability.

Official Secrets Acts (1911-1989)
Much information handled by Government Offices and even suppliers and customers of Government is covered by these Acts. Extreme caution must, therefore, be exercised before storing or transmitting any material which refers to national or international defence, intelligence, security or international relations. Heavy criminal penalties will be incurred if any user is in breach of the Act.

Libel Defamation Act (1996)
Libel and defamation are civil offences which can incur heavy financial penalties. As it is complicated it is one of the easiest laws to contravene through ignorance. Any facts which are published electronically, concerning individuals or organizations, (inclusive of opinions about them) must be accurate and verifiable. Views or opinions must not portray their subjects in any way which could damage their reputation.

Copyright Designs and Patents Act (1988)
Various Copyright, Designs and Patents Acts exist which protect the intellectual property of individuals. In general, these various Acts require that the permission of the owner of the intellectual property MUST be sought before any use of it is made whatsoever.

Code of Advertising Standards and Practice (1998)
It is not expected that any of WEBS electronic services would be used for placing and distribution of commercial advertisements although the platforms do advertise WEBS programmes, facilities, etc. However, if advertisements are placed then they must comply with the Code of Practice for Advertisers issued by the Advertising Standards Authority which requires in summary that all advertisements should be 'legal, decent, truthful and honest'.

Human Rights Act (1998)
Makes part of UK Law rights included under the European Convention on Human Rights: covers right to life; to marry; to education; private property; fair civil procedure; free election; freedom of thought; assembly; association; expression; religion; conscience; freedom from slavery; torture and discrimination. It should be noted that permission is required for publication of material and photographs in which the general public feature.

Regulation of Investigatory Powers Act (2000)
Specifies the framework governing the interception of electronic communications (data, fax, voice - inclusive of email.) on public and private networks : rules (Lawful Business Practice) permit such interception for purposes of investigation of unauthorised use (phones, email), checking of compliance to standards, monitoring of performance and functionality of systems, provision of evidence of business transactions.

Electronic Communications Act (2000)
Includes a directive on electronic signatures with regards to their use as evidence.

Terrorism Act (2000)
Includes provision for the trying of hackers under the terms of the Act.
NB. There is a general requirement in law against incitement of others to commit criminal acts and in some instances even to contemplate committing criminal acts. It should be noted therefore that any material published electronically which incites others to criminal acts or incites them to contemplate such acts is likely to be illegal.